Claims

What Is Claimed Is:

Sub B1

1. An information security system comprising:

a plurality of trusted authorities configurable in a rooted hierarchical structure including at least one of the trusted authorities being a superior authority and at least one of the trusted authorities being subordinate authorities; and

the superior authority operative to generate inter trusted authority trust modification data to dynamically vary validation starting authorities among the subordinate authorities.

2. The system of claim 1 wherein at least one of the subordinate authorities includes a certificate issuer operatively responsive to the inter trusted authority modification data for issuing certificates for at least one subscriber based on the inter trusted authority modification data.

3. The system of claim 1 wherein at least one of the subordinate authorities includes a subscriber trust anchor specifier, operatively responsive to the inter trusted authority modification data, that generates trust anchor modification data for a plurality of subscribers.

4. The system of claim 3 wherein the trust anchor modification data includes subordinate trust anchor data representing at least one trust anchor different from a local trust authority.

5. The system of claim 1 wherein the superior authority includes a trust anchor modification data certificate issuer that provides the trust anchor modification data as a signed data structure for the subordinate authorities.

6. The system of claim 1 wherein the trust anchor modification data includes data representing at least one of: scope of certification data, subordinate authority cross-certification allowance data, subordinate authority certification rule data, subordinate authority password rule data, subscriber trust anchor rule data and subscriber password rule data, certificate expiry policy, subscriber algorithm policy, and policy control message data.

7. The system of claim 1 wherein one of the trusted authorities is a root authority.

8. The system of claim 1 including subordinate authority memory containing data representing validation starting authority data, wherein the data is stored in response to receiving the inter trusted authority trust modification data.

9. An information security system comprising:

a plurality of trusted authorities configurable in a rooted hierarchical structure including at least one of the trusted authorities being a superior authority and at least one of the trusted authorities being subordinate authorities;

the superior authority operative to generate policy control message data to dynamically vary policy control data to facilitate trust authority policy delegation among the subordinate authorities wherein the policy control data includes inter trusted authority trust modification data to dynamically vary validation starting authorities among the subordinate authorities; and

wherein at least one of the subordinate authorities includes a certificate issuer operatively responsive to the inter trusted authority modification data for issuing certificates for at least one subscriber based on the inter trusted authority modification data and further includes a subscriber trust anchor specifier, operatively responsive to the inter trusted authority modification data, that generates trust anchor modification data for a plurality of subscribers.

10. The system of claim 9 wherein the trust anchor modification data includes subordinate trust anchor data representing at least one trust anchor different from a local trust authority.

11. The system of claim 10 wherein the superior authority includes a trust anchor modification data certificate issuer that provides the trust anchor modification data as a signed data structure for the subordinate authorities.

12. The system of claim 9 wherein the trust anchor modification data includes data representing at least one of: scope of certification data, subordinate authority cross-certification allowance data, subordinate authority certification rule data, subordinate authority password rule data, subscriber trust anchor rule data and subscriber password rule data, certificate expiry policy, subscriber algorithm policy, and policy control message data.

13. The system of claim 12 wherein one of the trusted authorities is a root authority.

14. The system of claim 13 including subordinate authority memory containing data representing validation starting authority data, wherein the data is stored in response to receiving the inter trusted authority trust modification data.

15. A method for providing information security comprising:

providing a plurality of trusted authorities configurable in a rooted hierarchical structure including at least one of the trusted authorities being a superior authority and at least one of the trusted authorities being subordinate authorities; and

generating inter trusted authority trust modification data to dynamically vary validation starting authorities among the subordinate authorities.

16. The method of claim 15 including issuing certificates for at least one subscriber based on the inter trusted authority modification data.

17. The method of claim 15 including generating trust anchor modification data for a plurality of subscribers.

18. The method of claim 17 wherein the trust anchor modification data includes subordinate trust anchor data representing at least one trust anchor different from a local trust authority.

19. The method of claim 15 including the step of providing the trust anchor modification data as a signed data structure for the subordinate authorities.

20. The method of claim 15 wherein the trust anchor modification data includes data representing at least one of: scope of certification data, subordinate authority cross-certification allowance data, subordinate authority certification rule data, subordinate authority password rule data, subscriber trust anchor rule data and subscriber password rule data, certificate expiry policy, subscriber algorithm policy, and policy control message data.

21. The method of claim 15 including the step of storing data representing validation starting authority data, in response to receiving the inter trusted authority trust modification data.